

Debunking Some Common Security Myths?

There is no one cause for these myths. They may have been formed because of a lack of information, an assumption, knowledge of a specific case that was then generalized, or some other source. As with any myth, they are passed from one individual to another, usually because they seem legitimate enough to be true. While believing these myths may not present a direct threat, they may cause you to be more relaxed about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.

What are some common myths, and what is the truth behind them?

- *Myth: Anti-virus software and firewalls are 100% effective.*
Truth: Anti-virus software and firewalls are important elements to protecting your information. However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.
- *Myth: Once software is installed on your computer, you do not have to worry about it anymore.*
Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities. You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.
- *Myth: There is nothing important on your machine, so you do not need to protect it.*
Truth: Your opinion about what is important may differ from an attacker's opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people.
- *Myth: Attackers only target people with money.*
Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage.
- *Myth: When computers slow down, it means that they are old and should be replaced.*
Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, hard drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware.